



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,689	04/23/2001	Stephen Sorkin	RECOP008	4377
21912	7590	02/03/2004	EXAMINER	
VAN PELT & YI LLP 10050 N. FOOTHILL BLVD #200 CUPERTINO, CA 95014			BAUM, RONALD	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 02/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/841,689

Applicant(s)

SORKIN ET AL.

Examiner

Ronald Baum

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1,2,5,8,10-12,16-19,21-25,27,28,31 and 34-36 is/are rejected.
- 7) ☒ Claim(s) 3,4,6,7,9,13-15,20,29,30,32,33 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
- a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6,7.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

Art Unit: 2135

DETAILED ACTION

1. Claims 1-36 are pending for examination.
2. Claims 1,2,5,8,10,11,12,16,17,18,19,21-25,27,28,31,34-36 are rejected.
Claims 3,4,6,7,9,13-15,20,29,30,32,33 are objected to.

Specification

The disclosure is objected to because of the following informalities: The attempt to incorporate subject matter into this application by reference to US patent applications only by a title (i.e., page 1, lines 17-21, "SYSTEM AND METHOD FOR COMPUTER SECURITY USING MULTIPLE CAGES", is improper because reference to said documents is incomplete without more specific identification (i.e., actual US patent applications numbers).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1,2,5,8,10-12,16-19,21,27 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran, U.S. Patent 6,647,400 B1.

Art Unit: 2135

4. As per claim 1; “A method for analyzing a logfile produced by a computer network security system [figure 3,8 and accompanying descriptions, col. 2,lines 40-55, col. 3,lines 40-51, col. 4,lines 24-36, col. 7,lines 42-49,lines 65-col. 8,line 23, col. 9,lines 15-21, col. 11,lines 28-54, col. 26,lines 57-col. 27,line 6, col. 33,lines 47-62, col. 35,lines 33-40], comprising: providing a regular expression query associated with a pattern to be searched for in the logfile [col. 12,lines 46-67, col. 23,lines 46-63, col. 41,lines 19-24]; and using the query to search for the pattern in the logfile. [col. 32,lines 49-col. 33,line 63, col. 34,lines 51-col. 35,line 46, col. 38,lines 30-col. 39,line 53]” ;

And further as per claim 27; “A system [This claim is the system (apparatus also, col. 3,lines 25-35) of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for analyzing a logfile produced by a computer network security system, comprising: a storage including a regular expression query associated with a pattern to be searched for in the logfile; and a processor configured to use the query to search for the pattern in the logfile.”;

And further as per claim 35; “A computer program product [This claim is the embodied software on computer readable media (also, col. 3,lines 25-35) of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for providing a regular expression query associated with a pattern to be searched for in the logfile; and using the query to search for the pattern in the logfile.”.

Art Unit: 2135

5. Claim 2 ***additionally recites*** the limitations that; “The method as recited in claim 1, wherein the pattern is associated with a possible sgid exploit.”. The teachings of Moran (col. 4, line 17-23 (sgid exploit is a type of buffer overflow attack), col. 33, lines 63-col. 34, line 68, col. 35, line 32-46, col. 36, lines 7-26) suggest such limitations.

And further as per claim 28; “The system as recited in claim 27 [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 2, and is rejected for the same reasons provided for the claim 2 rejection above], wherein the pattern is associated with a possible sgid exploit.”.

6. Claim 5 ***additionally recites*** the limitations that; “The method as recited in claim 1, wherein the pattern is associated with a possible suid exploit.”. The teachings of Moran (col. 4, line 17-23 (suid exploit is a type of buffer overflow attack), col. 33, lines 63-col. 34, line 68, col. 35, line 32-46, col. 36, lines 7-26) suggest such limitations.

And further as per claim 31; “The system as recited in claim 27 [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 5, and is rejected for the same reasons provided for the claim 5 rejection above], wherein the pattern is associated with a possible suid exploit.”.

7. Claim 8 ***additionally recites*** the limitations that; “The method as recited in claim 2, wherein the pattern is associated with processes spawned by a shell.”. The teachings of Moran (col. 26, lines 30-56) suggest such limitations.

8. Claim 10 ***additionally recites*** the limitations that; “The method as recited in claim 2, wherein the pattern is associated with user keystrokes, and the method further comprises aggregating the user keystrokes found in the logfile.”. The teachings of Moran (col. 26, lines 57-

Art Unit: 2135

col. 27, line 6 (where commands have been entered as keyboard “keystrokes”)) suggest such limitations.

9. Claim 11 *additionally recites* the limitations that; “The method as recited in claim 10, wherein the found user keystrokes are aggregated upon finding a keystroke representing a newline character.”. The teachings of Moran (col. 26, lines 57-col. 27, line 6 (where commands have been entered as keyboard “keystrokes”, and terminated with a newline character, and the aggregated command string is then processed, as is the case for UNIX based (i.e., col. 11, lines 28-40, col. 20, lines 65-67) systems)) suggest such limitations.

10. Claim 12 *additionally recites* the limitations that; “The method as recited in claim 11, further comprising presenting the aggregated keystrokes to a second user.”. The teachings of Moran (col. 7, lines 42-49, col. 10, lines 44-55) suggest such limitations.

11. Claim 16 *additionally recites* the limitations that; “The method as recited in claim 1, wherein the pattern is associated with files to be monitored.”. The teachings of Moran (col. 4, lines 1-8, col. 27, lines 30-col. 33, line 47) suggest such limitations.

12. Claim 17 *additionally recites* the limitations that; “The method as recited in claim 2, wherein using the query to search for the pattern includes searching for entries showing that a monitored file has been accessed.”. The teachings of Moran (col. 4, lines 1-8, col. 27, lines 30-col. 33, line 47) suggest such limitations.

13. Claim 18 *additionally recites* the limitations that; “The method as recited in claim 17, further comprising indicating to a second user a filename of the accessed monitored file.”. The teachings of Moran (col. 7, lines 42-49, col. 10, lines 44-55) suggest such limitations.

Art Unit: 2135

14. Claim 19 *additionally recites* the limitations that; “The method as recited in claim 17, further comprising indicating to a second user a process ID of a process that accessed the monitored file.”. The teachings of Moran (col. 7, lines 42-49, col. 10, lines 44-55) suggest such limitations.

15. Claim 21 *additionally recites* the limitations that; “The method as recited in claim 2, wherein using the query to search for the pattern includes searching for entries showing that an attempt has been made to access a monitored file.”. The teachings of Moran (col. 7, lines 42-49, col. 10, lines 44-55) suggest such limitations.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

16. Claims 22-25, 34 and 36 are rejected under 35 U.S.C. 102(b) as being anticipated by Lermuzeaux et al, U.S. Patent 5,621,889.

17. As Per claim 22; “A method for providing security for a computer network [ABSTRACT, ‘detecting intrusions and suspect users’, col. 1, lines 10-25, col. 2, lines 9-56], comprising: generating content sets for a computer associated with the network [ABSTRACT, ‘modeling the computer installation, its users, and their respective behavior’]; determining whether a user should be routed to the generated content sets [ABSTRACT, ‘comparing the modeled behavior of the system and of its users relative to modeled normal behavior’, col. 3, lines 29-60]; selecting one of the content sets if it is determined that the user should be routed

Art Unit: 2135

to the generated content sets; routing the user to the selected generated content set; producing a logfile of at least a portion of the user's activity with respect to the computer; and using at least one regular expression query to analyze the logfile. [ABSTRACT, col. 4, lines 44-col. 5, line 27]”;

And further as per claim 34; “A system [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 22, and is rejected for the same reasons provided for the claim 22 rejection above] for providing security for a computer network, comprising: a computer configured to generate content for the computer, wherein the computer is associated with the network; a network device configured to determine whether a user should be routed to the generated content and to, route the user to the generated content if it is determined that the user should be routed to the generated content; a logging mechanism configured to produce a logfile of at least a portion of the user's activities with respect to the generated content; and a storage including a regular expression query usable by the computer to search the logfile for a pattern associated with the regular expression query.”;

And further as per claim 36; “A computer program product [This claim is the embodied software on computer readable media (also, col. 3, lines 25-35) of the method claim 22, and is rejected for the same reasons provided for the claim 22 rejection above] for providing security for a computer network, comprising a computer usable medium having machine readable code embodied therein for generating content sets for a computer associated with the network; determining whether a user should be routed to the generated content sets; selecting one of the content sets if it is determined that the user should be routed to the generated content sets; routing the user to the selected generated content set; producing a logfile of at least a portion of

Art Unit: 2135

the user's activity with respect to the computer; and using at least one regular expression query to analyze the logfile.”;

18. Claim 23 *additionally recites* the limitations that; “The method as recited in claim 22, further comprising associating each generated content set with a virtual computer.”. The teachings of Lermuzeaux et al (col. 8, lines 6-12, 16-20, 56-col. 9, line 16 (“create an image in time and in space of the behavior *state* of the target as constituted by the computer installation”), col. 9, lines 7-17, 63-col. 10, line 11, col. 16, lines 23-34, col. 18, lines 25-30) suggest such limitations.

19. Claim 24 *additionally recites* the limitations that; “The method as recited in claim 23, wherein selecting one of the content sets includes choosing a content set associated with a virtual computer requested to be accessed by the user.”. The teachings of Lermuzeaux et al (col. 8, lines 6-12, 16-20, 56-col. 9, line 16 (“create an image in time and in space of the behavior *state* of the target as constituted by the computer installation”), col. 9, lines 7-17, 63-col. 10, line 11, col. 16, lines 23-34, col. 18, lines 25-30) suggest such limitations.

20. Claim 25 *additionally recites* the limitations that; “The method as recited in claim 24, wherein producing the logfile includes storing information regarding the user's activity with respect to the selected content set and associated virtual computer.”. The teachings of Lermuzeaux et al (col. 8, lines 6-12, 16-20, 56-col. 9, line 16 (“create an image in time and in space of the behavior *state* of the target as constituted by the computer installation”), col. 9, lines 7-17, 63-col. 10, line 11, col. 16, lines 23-34, col. 18, lines 25-30) suggest such limitations.

Art Unit: 2135

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

21. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lermuzeaux et al, U.S. Patent 5,621,889, as applied to claims 22 above, and further in view of Moran, U.S. Patent 5,991,410.

As per claim 26; "The method as recited in claim 25, wherein the computer is running on a Solaris operating system." ;

As recited in the claim 22 rejection above, Lermuzeaux et al teaches of a "Facility for detecting intruders and suspect callers in a computer installation and a security system including such a facility", etc., utilizing computer systems part of a computer network, utilizing associated operating systems with associated database and expert analysis, and database access software applications.

Moran is directed to a system and method for analyzing Solaris based operating system (col. 19, lines 49-65, col. 20, lines 49-67) file systems (database, etc.) to detect intrusions utilizing rule based and expert systems for said database access and analysis (col. 38, lines 13-65). Thus, one of ordinary skill in the art would have been motivated to include the Solaris based operating system invention of Moran with the Lermuzeaux et al IDS system to allow such database search/analysis using such a large scale operating environment for the Lermuzeaux et al IDS

Art Unit: 2135

system analysis engine functions. Such motivation to combine is recited by Moran (again, col. 38, lines 13-65).

Allowable Subject Matter

22. Claims 3, 4, 6, 7, 9, 13, 14, 15, 20, 29, 30, 32, 33 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim 3 ***additionally recites*** the limitations that; “The method as recited in claim 2, wherein using the query to search for the pattern includes searching for entries showing that a process has been started with effective group ID equal to zero.”;

And further as per claim 29; “The system as recited in claim 28 [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 3], wherein the processor is further configured to search for entries showing that a process has been started with effective group ID equal to zero.”;

Claim 4 ***additionally recites*** the limitations that; “The method as recited in claim 3, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID.”;

And further as per claim 30; “The system as recited in claim 29 [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 4], wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.”;

Art Unit: 2135

Claim 6 *additionally recites* the limitations that; “The method as recited in claim 5, wherein using the query to search for the pattern includes searching for entries showing that a process has been started with effective user ID equal to zero.”.

And further as per claim 32; “The system as recited in claim 31 [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 6], wherein the processor is further configured to search for entries showing that a process has been started with effective user ID equal to zero.”;

Claim 7 *additionally recites* the limitations that; “The method as recited in claim 6, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID.”;

And further as per claim 33; “The system as recited in claim 32 [This claim is the system (apparatus also, col. 3, lines 25-35) of the method claim 7], wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.”;

Claim 9 *additionally recites* the limitations that; “The method as recited in claim 8, wherein using the query to search for the pattern includes searching for entries showing that the shell has started a process, storing a process ID of the process, and searching for entries showing processes with parent process ID equal to the stored process ID.”;

Claim 13 *additionally recites* the limitations that; “The method as recited in claim 2, wherein the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile.”;

Art Unit: 2135

Claim 14 *additionally recites* the limitations that; "The method as recited in claim 13, wherein the found screen output characters are aggregated upon finding a screen output character representing a newline character.";

Claim 15 *additionally recites* the limitations that; "The method as recited in claim 14, further comprising presenting the aggregated keystrokes to a second user.";

Claim 20 *additionally recites* the limitations that; "The method as recited in claim 19, further comprising automatically searching for the process ID in the logfile.";

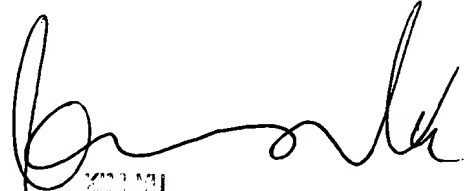
Conclusion

23. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu, can be reached at (703) 305-4393. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100